**Practical No. 2**

**Data Acquisition tool (Write Blocker)**

1. USB Write Blocker
2. SATA Write Blocker

**USB Write Blocker**

Digital evidence is our major issue of concern in Forensic investigation. Forensic investigators need to absolutely assure of the fact that the data they obtain as digital evidence is not altered during the capture, analysis, and control. In the courtroom everyone including attorneys, judges, jurors need to feel confident that digital evidence has not been tampered and is legitimate. How can you be assured that digital evidence has not tampered?

According to the **NIST-National Institute of Standards and Technology**, the investigator follows a certain set of rules and procedures to prevent the execution of any program that might modify the contents of the disk.

Some of these procedures are:

* Use an operating system and other software that is trusted to not to write anything to the disk without any explicit instruction.
* Use hard disk write block tools to prevent any hard disk writes.
* Wherever possible, set a hardware jumper to make the disk read-only.

**Diagram**



**Introduction:-**

Write Blocker is a tool designed to prevent any write access to the hard disk, thus permitting read-only access to the data storage devices without compromising the integrity of the data. A write blocking if used correctly can guarantee the protection of the chain of custody. NIST has issued a set of general guidelines for write blocking requirements:

1. The write-blocker tool shall not allow a protected drive to be changed.
2. The write-blocker tool shall not prevent any operations to a drive that is not protected.
3. The write-blocker tool shall not prevent obtaining any information from or about any drive.

**Types of Write Blocker:**

**Hardware Write Blocker and Software Write Blocker.** Both types of write blockers are meant for the same purpose that is to prevent any writes to the storage devices. Let’s discuss each type of write blocker in detail.

**Hardware write blockers** are used to intercept and block any modifying command from ever reaching the storage device. Some of its features include:

* They offer monitoring and filtering any activity that is transmitted or received between its interface connections to the computer and the storage device.
* They provide built-in interfaces to a number of storage devices.
* Hardware write blockers can connect to other types of storage with adapters.
* Hardware devices that write block also provide a visual indication of function through LEDs and switches. This makes them easy to use and makes functionality clear to users.

**The software blocker** is an application that is run on the operating system that implements a software control to turn off the write capability of the operating system. If you are using a software write blocker, ensure to attach the external evidence collection drive prior to activating the software blocker as this will allow the external drive to be written to.

* If you are collecting data from a USB device such as a thumbdrive, you need to activate the software or hardware blocker prior to connecting the device to the collection system. Importantly, make sure that you have already connected the external evidence collection drive and prepared it.

**SATA Write Blocker**



A **forensic disk controller** or hardware write-block device is a specialized type of computer hard disk controller made for the purpose of gaining read-only access to computer hard drives without the risk of damaging the drive's contents.

Go for a write blocker that allows the switching for the sake of convenience in the cases where you need to connect to a SATA or IDE Drives.